認証報告書

独立行政法人 情報処理推進機構
理事長 西垣 浩司
原 紙
押印済

評価対象

申請受付日（受付番号）	**平成**20**年**2**月**22**日** (IT**認証**8201)
認証番号	C0197
認証申請者	**富士ゼロックス株式会社**
TOE**の名称**	EP**通信集約サーバーソフトウエア**
TOE**のバージョン**	1.0.1
PP**適合**	**なし**
適合する保証パッケージ	EAL2
開発者	**富士ゼロックス株式会社**
評価機関の名称	**有限責任中間法人** IT**セキュリティセンター 評価部**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成20年11月28日

セキュリティセンター 情報セキュリティ認証室
技術管理者 鈴木 秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 改訂第1版 (翻訳第1.2版)

② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第1版 (翻訳第1.2版)

評価結果：合格

「EP通信集約サーバーソフトウエア」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「EP通信集約サーバーソフトウエア」（以下「本TOE」という。）について有限責任中間法人 ITセキュリティセンター 評価部（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である富士ゼロックス株式会社に報告するとともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、EPサービスの提供を受ける富士ゼロックス株式会社製複合機の利用者を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL2適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：	EP通信集約サーバーソフトウエア
バージョン：	1.0.1
開発者：	富士ゼロックス株式会社

1.2.2 製品概要

TOEであるEP通信集約サーバーソフトウエアを搭載したサーバーは、富士ゼロックス株式会社（以下「FX」という。）がFX製のEP-BB機能搭載複合機の利用者に対して提供するEPサービスにおいて、EPサービスの提供を受ける利用者側に設

置され、EPサービスの対象となるEP-BB機能搭載複合機とEPサービスの提供のためにFXが管理運用しているEPセンターとの間の通信を中継する。

TOEは、PC上で稼動するアプリケーションソフトウェアであり、EP-BB機能搭載複合機とインターネット上のEPセンターとの間でTOEが中継する通信データを保護するために、通信データの盗聴と改ざんや通信相手のなりすましを防止するためのセキュリティ機能とその管理機能を提供する。

1.2.3 TOE範囲とセキュリティ機能

1) TOEの範囲

TOEの運用環境を図1-1に示す。図1-1において、通信中継サーバー(PC)がTOEを搭載したサーバーであり、TOEは通信中継サーバー(PC)のアプリケーションソフトウェア部分である。

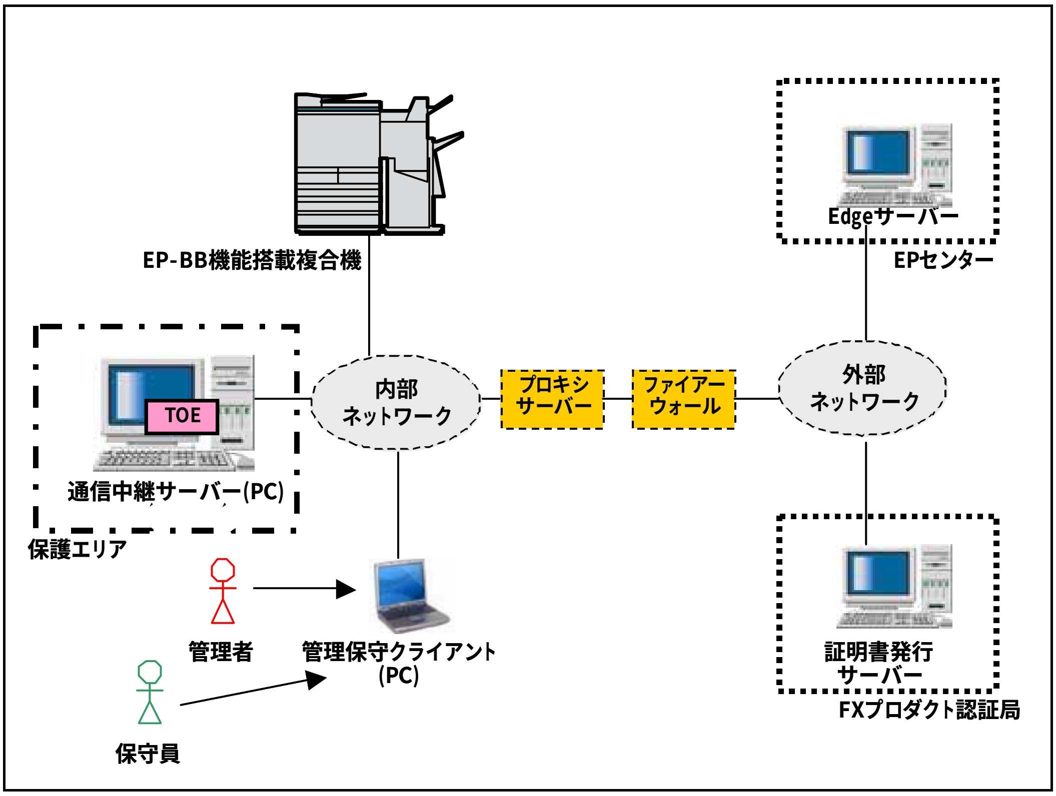


図1-1　TOEの運用環境

通信中継サーバー(PC)の基本的な動作は、EP-BB機能搭載複合機からの通信を中継し、外部ネットワークにあるEPセンターのEdgeサーバーと通信することである。通信にはHTTPSプロトコルを使用し、HTTPSプロトコルにおいてTOEがあらかじめ必要とするTOE自身の証明書や認証局の証明書は、FXプロダクト認証局にある証明書発行サーバーからTOEが自動的に取得する。また、TOEの利用

者である管理者と保守員が、Webブラウザを搭載した端末である管理保守クライアント(PC)を操作して、TOEの設定等を行う管理機能を備えている。

通信中継サーバー(PC)のソフトウェア構成を図1-2に示す。図1-2で、TOEの範囲は、点線で囲まれたソフトウェア部分である。なお、図1-2ではIT環境のプロキシサーバー、ファイアーウォール、証明書発行サーバーは省略されている。

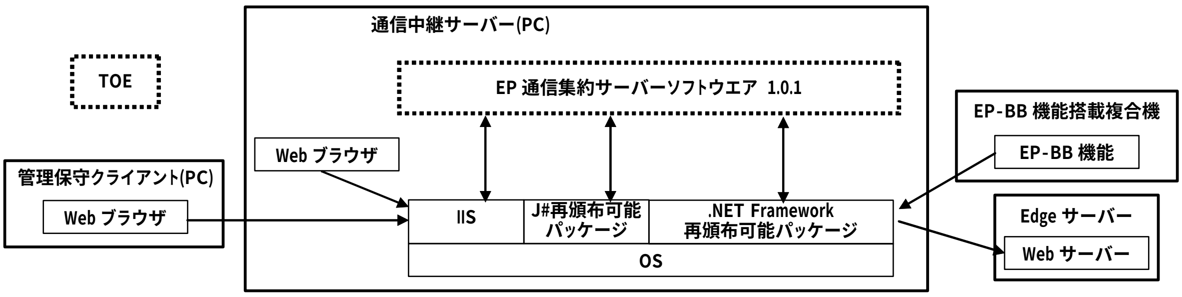


図1-2　TOE**の範囲**

TOEは、「.NET Framework 再頒布可能パッケージ」を実行環境として動作するアプリケーションソフトウェアである。TOEは、HTTPSプロトコルによる通信中継を「.NET Framework 再頒布可能パッケージ」で提供されるライブラリ機能を使って実装している。TOEは、EP-BB機能搭載複合機に対してはHTTPSサーバーとして動作し、Edgeサーバーに対してはHTTPSクライアントとして動作する。HTTPSプロトコルによる通信中継においてTOE自身が行っている処理は、中継する通信データの送受信のために「.NET Framework 再頒布可能パッケージ」で提供されるHTTPSプロトコル処理を呼び出す部分と、HTTPSプロトコルによる通信開始時に通信相手のEP-BB機能搭載複合機及びEdgeサーバーから提示される証明書の正当性を検証する部分である。

Webサーバーソフトウェアである「IIS」は、管理保守クライアント(PC)のWebブラウザに対してTOEが管理機能を提供するために使われており、HTTPSプロトコルによる通信中継には使用されない。なお、管理保守クライアント(PC)のWebブラウザの代用として通信中継サーバー(PC)上のWebブラウザを使用することもできる。また、TOEは「J#再頒布可能パッケージ」で提供されるファイル圧縮機能を利用して監査ログファイルの圧縮を行っている。

2) TOEのセキュリティ機能

TOEは、中継するEP通信データを保護するために以下のセキュリティ機能を提供する。

(1) HTTPS通信中継機能

EP通信データの盗聴や改ざんを防止するために、TOEは、EP-BB機能搭載複合機からEdgeサーバーへの通信の中継に、暗号化通信プロトコルである

HTTPSプロトコルを適用して通信を行う。また、EP-BB機能搭載複合機やEdgeサーバーへのなりすましによるEP通信データの不正な送受信を防止するために、TOEは、HTTPSプロトコルによる通信開始の際に、通信相手から提示された証明書の正当性を検証し、正当な通信相手との通信を許可する。さらに、TOEは、証明書発行サーバーから証明書を取得する際に、TOEが信頼する以外の認証局から発行された不正な証明書を取得してしまうことを防止するために、証明書発行サーバーの正当性を検証し、正当な証明書発行サーバーから証明書を取得する。

(2) 利用者識別認証機能

TOEの設定等の管理機能が許可なく利用されることを防止するために、TOEは利用者の識別認証を行い、利用者に応じてアクセスを制限する。

(3) ログ生成/ダウンロード機能

(1)(2)のセキュリティ機能を確実に実施する上で侵害事象を検出できるようにするために、TOEは監査ログを生成し、利用者が生成された監査ログを管理保守クライアント(PC)にダウンロードする機能を提供する。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「EP通信集約サーバーソフトウエア セキュリティーターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、本TOEの開発・製造・出荷環境がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「富士ゼロックス株式会社 EP通信集約

サーバーソフトウエア 評価報告書」(以下「評価報告書」という。)[13]に示されている。なお、評価方法は、CEM([11][12]のいずれか)に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年11月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅 威
T.EP_COM	<外部ネットワーク上での保護資産の漏洩、改ざん> 外部ネットワーク上の攻撃者が、プロトコルアナライザを使用し、TOEとEdgeサーバーとの間で送受信されるEP通信データを盗み見るかもしれない。また、EP通信データを改ざんし、TOEが送信したデータとは異なったデータをEdgeサーバーに受信させるかもしれない。
T.FAKE_EDGE_SERVER	<Edgeサーバーになりすまし> 攻撃者が偽Edgeサーバーを立ち上げ、その偽Edgeサーバーの攻撃者が外部ネットワークを介して、EP通信データに不正にアクセスするかもしれない。
T.FAKE_EP-BB_DEVICE	<EP-BB機能搭載複合機になりすまし> 攻撃者が偽EP-BB機能搭載複合機を内部ネットワークに設置し、EP通信データに不正にアクセスするかもしれない。
T.ACCESS_TSF_DATA	<TSFデータへの不正アクセス> 攻撃者が、管理保守クライアント(PC)のWebブラウザから、管理者または保守員のみアクセス許可されているTOE設定データにアクセスして設定を変更するかもしれない。 また、ログをダウンロードするかもしれない。
T.CE_ACCESS	<CEによる不正アクセス> 保守員、または保守員になりすました者が、管理者の許可なく、管理者または保守員のみアクセス許可されているTSFデータにアクセスして設定を変更するかもしれない。 また、ログをダウンロードするかもしれない。

(注) EP通信データには課金のための情報、ログにはIPアドレス等の利用者側の内部情報、TOE設定データにはセキュリティ機能に影響する情報が含まれており、脅威に対する保護を必要とする。

2.1.2 組織のセキュリティ方針

本TOEの利用に当たって要求される組織のセキュリティ方針はない。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-2に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表2-2 TOE使用の前提条件

識別子	前提条件
A.PHYSICAL	<物理的な保護> 通信中継サーバー(PC)は、許可された利用者のみが入場可能な場所に設置され、入場が許可された利用者だけが物理的にアクセスすると仮定する。
A.ADMIN	<信頼できる管理者> 管理者、及び複合機管理者は、課せられた役割を遂行するために必要な知識と能力を有し、悪意をもった不正を行わないと仮定する。
A.PASSWORD	<守られたパスワード> 管理者が、管理保守クライアント(PC)からTOEにアクセスする際には、パスワードが漏洩しないと仮定する。 管理者パスワードと複合機管理者パスワードは、常に厳重に管理され、漏洩しないと仮定する。
A.NET	<盗聴から守られた内部ネットワーク> TOE、EP-BB機能搭載複合機、及び管理保守クライアント(PC)を設置する内部ネットワークは盗聴されない環境を構築すると仮定する。
A.FIREWALL	<外部から守られた内部ネットワーク> TOE、EP-BB機能搭載複合機、及び管理保守クライアント(PC)を設置する内部ネットワークは、ファイアーウォールによって外部ネットワークから隔離され、外部ネットワークからの攻撃から保護されると仮定する。
A.DEVICE	<守られた複合機> 複合機管理者だけが、EP-BB機能搭載複合機のEP通信データの元となるデータにアクセスできると仮定する。
A.SERVER_PC	<守られた通信中継サーバー(PC)>

	通信中継サーバー（PC）上のOSには、許可された者だけがアクセスできると仮定する。
A.CLIENT_PC	<守られた管理保守クライアント(PC)> 管理保守クライアント(PC)上にあるログ情報が漏洩しないと仮定する。

(注) A.FIREWALLの「外部ネットワークから隔離」とは、内部ネットワークがファイアーウォールを境界として外部ネットワークと接続され、その間で必要な通信以外はファイアーウォールの設定によって遮断されていることを意図している。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。利用者は、前提条件を満たすため下記ドキュメントの内容の十分な理解と遵守が要求される。

・管理者向け
EP通信集約サーバーソフトウエア取扱説明書 2008年8月 第1版
(帳票No:ME4226J1-2)

・保守員向け
EP通信集約サーバーソフトウエア取扱説明書(保守員向け補足情報) K1.02

2.1.5 構成条件

本TOEは、PC上で稼動するアプリケーションソフトウェアである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

TOEが稼動する通信中継サーバー(PC)のハードウェア構成を表2-3に示す。また、TOE以外のソフトウェア構成を表2-4に示す。

TOEは、通信中継サーバー(PC)と管理保守クライアント(PC)について複数のバージョンのソフトウェアに対応している。その中で、評価対象となるソフトウェア構成組合せは、表2-5に示す6通りである。なお、管理保守クライアント(PC)のハードウェアは、表2-5に示すソフトウェアが動作するPCであれば良い。

表2-3　通信中継サーバー(PC)のハードウェア構成

項目	仕様	備考
機種	PC/AT 互換機	ネットワークポート (10/100/1000Base-T)必要
CPU	1GHz 以上のプロセッサ	
メモリ	512MB 以上	

ハードディスク空き容量	1GB 以上	
ディスプレイ	PC/AT 互換機に接続可能な仕様	TOE のインストール時に必要
外部記憶装置	CD-ROM ドライブ	TOE のインストール時に必要
キーボード・マウス	PC/AT 互換機に接続可能な仕様	

表2-4　通信中継サーバー(PC)のソフトウェア構成

項目	名称	備考
OS	以下のいずれかの OS。 ・Windows Server 2003, Standard Edition R2 日本語版 ・Windows XP Professional 日本語版 SP2 ・Windows Vista Business 日本語版	
IIS	IIS（OS に附属するバージョン）	Web サーバーソフトウェア。
J#再頒布可能パッケージ	Microsoft Visual J# 2.0 再頒布可能パッケージ	本 TOE は、本パッケージの中のファイル圧縮用のライブラリを使用する。
.NET Framework 再頒布可能パッケージ	Microsoft .NET Framework 2.0 再頒布可能パッケージ または Microsoft .NET Framework 3.0 再頒布可能パッケージ	本 TOE の実行環境。 本 TOE はバージョン 2.0 の機能だけを使用しており、その機能を包含するバージョン 3.0 でも動作する。 ただし評価は以下のバージョンで行う。 ・OS が Windows Vista の場合は、OS に標準搭載されているバージョン 3.0。 ・それ以外の OS の場合は、本 TOE と共に再頒布されるバージョン 2.0。

表2-5　評価対象のソフトウェア構成組合せ(6通り)

No.	通信中継サーバー(PC)		管理保守クライアント(PC)		通信プロトコル
	OS	IIS	OS	Web ブラウザ	
1	Windows Server 2003, Standard Edition R2 日本語版	IIS6.0	Windows XP Professional 日本語版 SP2	Microsoft Internet Explorer 6 SP2	IPv4
2	Windows Server 2003, Standard	IIS6.0	Windows XP Professional 日本語版	Windows Internet	IPv4

	Edition R2 日本語版		SP2	Explorer 7	
3	Windows XP Professional 日本語版 SP2	IIS5.1	Windows XP Professional 日本語版 SP2	Microsoft Internet Explorer 6 SP2	IPv4
4	Windows XP Professional 日本語版 SP2	IIS5.1	Windows XP Professional 日本語版 SP2	Windows Internet Explorer 7	IPv4
5	Windows Vista Business 日本語版	IIS7.0	Windows Vista Business 日本語版	Windows Internet Explorer 7	IPv4
6	Windows Vista Business 日本語版	IIS7.0	Windows Vista Business 日本語版	Windows Internet Explorer 7	IPv6

(注) 通信中継サーバー(PC)には、上記のソフトウェアの他に、表2-4に示す「J#再頒布可能パッケージ」と「.NET Framework再頒布可能パッケージ」が含まれる。

2.2 セキュリティ対策

本TOEは、2.1.1の脅威に対抗するために以下のセキュリティ機能を具備する。

(1) HTTPS通信中継機能

本機能は、脅威T.EP_COM(外部ネットワーク上での保護資産の漏洩、改ざん)、T.FAKE_EDGE_SERVER(Edge サーバーになりすまし)、及びT.FAKE_EP-BB_DEVICE(EP-BB機能搭載複合機になりすまし)に対抗する機能である。

TOEは、EP-BB機能搭載複合機とEdgeサーバーとの通信を中継する際に、.NET Framework再頒布可能パッケージの機能を利用して、通信データを暗号化するHTTPSプロトコルを適用する。また、TOEは、HTTPSプロトコルによる通信開始時に、EP-BB機能搭載複合機及びEdgeサーバーから提示される証明書の正当性を、TOEがあらかじめ取得しておいた認証局の証明書を使って検証し、正当性の検証された通信相手との通信を許可する。これにより、通信データの盗聴と改ざんや通信相手のなりすましを防止する。

さらに、TOEは、上記の機能を補助するために、次の機能を提供する。

TOEは、証明書発行サーバーから認証局の証明書及びTOE自身の証明書を取得する際にも、HTTPSプロトコルを使用して通信相手から提示される証明書の正当性を検証し、正当性の検証された証明書発行サーバーから必要な証明書を取得する。その際の証明書発行サーバーの証明書の検証は、TOEがあらかじめ保持し

ている証明書のハッシュ値や証明書発行サーバーの情報を用いて行う。これにより、TOEが信頼していない認証局から発行された証明書を取得することを防止する。

　また、TOEは、EP-BB機能搭載複合機からの通信を受信するための通信ポート番号を設定する機能を、管理者及び保守員に提供する。

(2) 利用者識別認証機能

　本機能は、脅威T.ACCESS_TSF_DATA(TSFデータへの不正アクセス)、及びT.CE_ACCESS(CEによる不正アクセス)に対抗する機能である。

　TOEは、TOEにアクセスする利用者である管理者と保守員を識別認証し、利用者に応じてTOEの設定等を行う管理機能のアクセスを制限する。また、TOEは、管理者が許可していない間は保守員のログインを禁止する機能を管理者に提供する。これにより、セキュリティのふるまいに影響を与えるデータが管理者の許可なく変更されることを防止する。

　さらに、TOEは、上記の機能を補助するために、次の機能を提供する。

　TOEは、利用者のパスワード変更時にパスワード文字列が一定の基準を満たすことを要求する。また、利用者が規定時間内に連続して認証に失敗した場合、一定時間、識別認証を拒絶する。これにより、識別認証のためのパスワードが、実用的な期間内に推測されることを防止する。

(3) ログ生成/ダウンロード機能

　本機能は、HTTPS通信中継機能及び利用者識別認証機能を補助する機能であり、それらのセキュリティ機能を確実に実施する上で侵害事象を検出できるようにするための機能である。

　TOEは、HTTPS通信中継機能や利用者識別認証機能に関して監査ログを生成する。監査ログを格納する領域が満杯の場合には古いログファイルを削除して新しい監査ログを記録する。また、生成された監査ログを管理保守クライアント(PC)にダウンロードする機能を管理者及び保守員に提供する。この機能を利用して、管理者及び保守員は定期的に監査ログを検査することで、セキュリティ機能の侵害を早期に検出することができる。

3 評価機関による評価実施及び結果

3.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年3月に始まり、平成20年11月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年7月に開発・製造現場、及び配送現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20年6月及び同年7月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成を図3-1　開発者テストの構成図に示す。

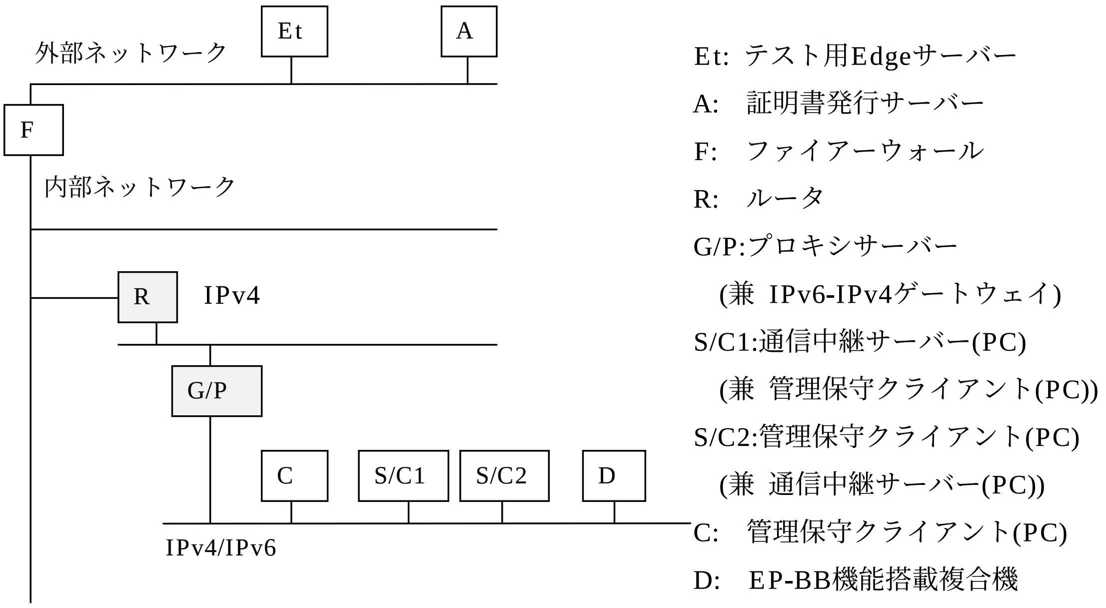


図3-1　開発者テストの構成図

図3-1において、使用している機器の構成を表3-1、表3-2、表3-3、及び表3-4に示す。それらの表では、テスト用Edgeサーバー、証明書発行サーバー、ファイアーウォール及びルータは省略されている。

開発者テストでは、表3-3に示す6通りのソフトウェア環境をテストするために、図3-1のS/C1、S/C2、Cを表3-4に示す組合せで使用している。通信中継サーバー(PC)としては、S/C1またはS/C2のいずれか一台を使用する。管理保守クライアント(PC)としては、管理保守クライアント(PC) が2台の場合のテストに対応するために、S/C1、S/C2、Cのうち2台を使用する。ただし、S/C1とS/C2で管理保守クライアント(PC)を構成するにあたっては、仮想マシン環境を実現するソフトウェアであるVMwareを使用し、VMwareで提供される仮想マシン上にOSを含むソフトウェア環境を構築している。

また、G/Pはプロキシサーバーの機能の他にIPv6とIPv4のTCPを中継変換するゲートウェイ機能を備えている。

開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。なお、テスト用EdgeサーバーやVMwareを使用した管理保守クライアント(PC)の構成は、TOEと通信するソフトウェアは運用環境と同じであり、STの構成と同等であることが評価者により確認されている。

表3-1　通信中継サーバー(PC)兼管理保守クライアント(PC)の構成

項目		S/C1、S/C2
ハードウェア	機種名	PC/AT互換機
	CPU	Intel Core2 Duo E6400 (2.13GHz)
	メモリ	3GB
	ハードディスク空き容量	46GB
	その他	10/100/1000Base-Tネットワークポート内蔵、17型液晶ディスプレイ、DVD-ROMドライブ、USBキーボード、USBマウス
ソフトウェア		「表3-3 ソフトウェア環境」に示す通信中継サーバー(PC)と管理保守クライアント(PC)のソフトウェアを「表3-4 ソフトウェア環境と使用機器」に示す組合せで構成。

表3-2　各種機器構成

項目	G/P	D	C
機種名	PC/AT互換機	DocuCentre-Ⅲ3000	PC/AT互換機
CPU	Intel Celeron (2GHz)	―	Intel Core2 Duo E6400 (2.13GHz)
メモリ	512MB	―	2GB
ソフトウェア(OS)	FreeBSD 6.2-RELEASE	―	「表3-3 ソフトウェア環境」に示す管理保守クライアント(PC)のソフトウェアを「表3-4 ソフトウェア環境と使用機器」に示す組合せで構成。
その他ソフトウェア	Proxy: Squid 2.6-STABLE IPv6-to-IPv4 TCP中継変換: faith	―	

表3-3　ソフトウェア環境

<table>
<tr><th rowspan="2">パタン</th><th colspan="4">通信中継サーバー(PC)</th><th colspan="2">管理保守クライアント(PC)</th><th rowspan="2">通信プロトコル</th></tr>
<tr><th>OS</th><th>IIS</th><th>J#再頒布可能パッケージ</th><th>.NET Framework 再頒布可能パッケージ</th><th>OS</th><th>ブラウザ</th></tr>
<tr><td>1</td><td>Windows Server 2003, Standard Edition R2 日本語版</td><td>IIS6.0</td><td rowspan="6">Microsoft Visual J# 2.0再頒布可能パッケージ</td><td rowspan="4">Microsoft .NET Framework 2.0 再頒布可能パッケージ</td><td>Windows XP Professional 日本語版 SP2</td><td>Microsoft Internet Explore 6.0 Service Pack 2</td><td>IPv4</td></tr>
<tr><td>2</td><td>Windows Server 2003, Standard Edition R2 日本語版</td><td>IIS6.0</td><td>Windows XP Professional 日本語版 SP2</td><td>Windows Internet Explore® 7</td><td>IPv4</td></tr>
<tr><td>3</td><td>Windows XP Professional 日本語版 SP2</td><td>IIS5.1</td><td>Windows XP Professional 日本語版 SP2</td><td>Microsoft Internet Explore 6.0 Service Pack 2</td><td>IPv4</td></tr>
<tr><td>4</td><td>Windows XP Professional 日本語版 SP2</td><td>IIS5.1</td><td>Windows XP Professional 日本語版 SP2</td><td>Windows Internet Explore 7</td><td>IPv4</td></tr>
<tr><td>5</td><td>Windows Vista Business 日本語版</td><td>IIS7.0</td><td rowspan="2">Microsoft .NET Framework 3.0 再頒布可能パッケージ</td><td>Windows Vista Business 日本語版</td><td>Windows Internet Explore 7</td><td>IPv4</td></tr>
<tr><td>6</td><td>Windows Vista Business 日本語版</td><td>IIS7.0</td><td>Windows Vista Business 日本語版</td><td>Windows Internet Explore 7</td><td>IPv6</td></tr>
</table>

表3-4　ソフトウェア環境と使用機器

ソフトウェア環境パタン	通信中継サーバー(PC)	管理保守クライアント(PC) (以下の2台を使用)	
1	S/C1	S/C1(VMware)	S/C2(VMware)
2	S/C1	S/C2	S/C1(VMware)
3	S/C2	S/C1	S/C2(VMware)
4	S/C1	S/C2	S/C1(VMware)
5	S/C2	C	S/C1(VMware)
6	S/C2	C	S/C1(VMware)

※表3-4は表3-3のソフトウェア環境の6つのパタンをどの機器で構成したかを示す。「VMware」の表示は該当するパタンの環境をVMwareを使用して仮想マシン上に構築したことを示す。表示のないものは、ハードウェア上に直接構築している。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

開発者テストは、表3-5に示すセキュリティ機能を刺激する手法及びセキュリティ機能のふるまいを観察する手法を使用して実施した。

表3-5　開発者テストのテスト手法

項目	使用したテスト手法	
セキュリティ機能を刺激する手法	管理保守クライアント(PC)の操作	開発証拠資料及びガイダンス文書の記述に基づき、管理保守クライアント(PC)を操作することにより、通信中継サーバー(PC)に搭載されたTOEを刺激する。管理保守クライアント(PC)の操作は、１台の場合と2台同時に使用した場合の2通り行う。
	EP-BB機能搭載複合機の操作	開発証拠資料及びガイダンス文書の記述に基づき、EP-BB機能搭載複合機を操作することにより、EP-BB機能搭載複合機から通信中継サーバー(PC)を経由したテスト用Edgeサーバーへの通信を行い、通信中継サーバー(PC)に搭載されたTOEを刺激する。
	通信中継サーバー(PC)のOSの操作	通信中継サーバー(PC)のOSの機能を使用して、TOEが使用するEP証明書ファイルを削除したり、時刻を設定したりすることにより、証明書の更新や時刻に関するセキュリティ機能を起動する。
セキュリティ	管理保守クライ	管理保守クライアント(PC)の画面等に出力されたふる

機能のふるまいを観察する手法	アント(PC)からの観察	まいの結果を目視により観察する。
	監査ログの観察	監査ログのデータからセキュリティ機能のふるまいを確認する。
	他IT製品からの観察	EP-BB機能搭載複合機及びテスト用Edgeサーバーの操作画面やデータから、EP-BB機能搭載複合機がTOEを介してEdgeサーバーと行う通信を確認する。
	通信中継サーバー(PC)のOSからの観察	EP証明書ファイルの存在やファイルの生成時刻情報をOSの機能により確認する。

b.　実施テストの範囲

テストは開発者によって165項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。また、STに記述されているソフトウェア構成6通りのすべての組合せにおいて、すべてのセキュリティ機能がテストされたことが検証されている。

c.　結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

3.3.2　評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

評価者が実施したテストの構成を図3-1に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

なお、評価者テストの構成と開発者テストの構成の違いを以下に示す。評価者テストの構成はSTの構成と同じであり、開発者テストの構成との違いはテストに影響がないことを評価者が確認している。

・EP-BB機能搭載複合機として、開発者テストではDocuCentre-III3000を使用し

ているが、評価者テストでは類似機種のApeosPortⅢC3300を使用している。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

・開発者テストのサンプルを使用したテスト

TOEが、開発者がテストしたとおりにふるまうことの確信を得るためのテストである。開発者が実施したテスト165項目から、すべてのセキュリティ機能及びすべてのインタフェースが含まれるように考慮し、43のテスト項目を選択した。ソフトウェア構成の組合せは、開発者テストと同じ構成を使用する。

・評価者が考案したテスト

開発者テストをふまえ、TOEが仕様のとおりにふるまうことの確信を得るためのテストである。開発者がテストしていないパラメタ値や複数の操作の組合せによるテスト項目を、すべてのセキュリティ機能及びすべてのインタフェースが含まれるように考慮し、10項目考案した。ソフトウェア構成の組合せは、6通りすべての組合せで、すべてのテストを実施する。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

・開発者テストのサンプルを使用したテスト

開発者テストと同じテスト手法を用いた。

・評価者が考案したテスト

開発者テストと同じテスト手法を用い、パスワード文字列の識別の境界条件、複数端末による同時操作、複数の設定項目の同時更新等、開発者テストではテストされていないパラメタ値や操作組合せをテストした。

さらに、開発者テストではテストされていないパラメタ値として、本TOEが信頼する認証局以外の認証局が発行した証明書（以下、「不正な証明書」という。）を使いテストを実施した。テストは次の2通り実施している。

1つは、EP-BB機能搭載複合機の代わりに不正な証明書を設定した「なりすまし用複合機」を使って本TOEに通信を試み、HTTPS通信のセッション確立が成功しないことを本TOEのログ情報で確認した。

もう1つは、Edgeサーバーの代わりに不正な証明書を設定した「なりすまし用Edgeサーバー」を使い、本TOEが通信を中継する際に、本TOEからなりすまし用Edgeサーバーに対するHTTPS通信のセッション確立が成功

しないことを本TOEのログ情報で確認した。

テストに使用した「なりすまし用複合機」及び「なりすまし用Edgeサーバー」の構成を表3-6に示す。いずれの機器も、目的のテストのために適切であることを評価者が確認している。

表3-6　不正な証明書のテストの使用機器

名称	ハードウェア	ソフトウェア
なりすまし用Edgeサーバー	Sun Blade 1000	OS：Sun Microsystems Solaris 8 7/01 ソフト：Apache HTTP Server 2.2.6
なりすまし用複合機	Panasonic Let's note CF-T7	OS：Windows XP SP2 ソフト：Java 6 Update 6、及びテスト用プログラム(HTTPSクライアントとしてセッション確立を行う)

c.　結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

3.3.3　評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1)　評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a.　懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

・Web関連の公知の脆弱性（バッファオーバフロー、コマンドやスクリプト注入等の不正入力による誤動作、URL直接指定による識別認証の回避)。
・何らかの方法でTOE自身に設定されている証明書が削除されたときに、証明書の更新がされずに予期しない動作をしてしまう可能性。
・複数端末からの設定が競合し、意図しない設定がされてしまう可能性。
・意図していないネットワークサービスの不正使用。

・プロトコルアナライザによる通信盗聴。
・トラフィック負荷によるセキュリティ機能の機能不全。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

・管理保守クライアント(PC)のWebブラウザを使用して、URLや各種入力に対して、制限値を越える文字数、OSコマンド、スクリプト、特殊文字、URLの直接指定等、脆弱性を引き起こす可能性のある文字列を入力し、Webブラウザに表示される画面を確認する。
・TOEが取得した証明書をOSの機能で削除し、その状態でTOEを動作させ、証明書が正常に更新されることをOS機能で確認する。
・2台の管理保守クライアント(PC)を使用し、１台の端末で管理項目の設定をしてその設定値を実際に反映させるためにTOEを再起動する間に、別の端末から同じ設定項目を別の設定値に変更し、設定を反映するために再起動をした前者の設定値が有効となることをTOEの動作で確認する。
・インターネットで入手できるポートスキャンツールnmapを搭載したPCを内部ネットワークに接続して、通信中継サーバー(PC)の全通信ポートをスキャンし、意図しない通信ポートが使用されていないことをツールの実行結果で確認する。
・インターネットで入手できるプロトコルアナライザツールwiresharkを搭載したPCを内部ネットワークに接続して、TOEからEdgeサーバーに対して送信されたデータを観測し、データが解析できないことを確認する。
・インターネットで入手できるIPパケット生成送信ツールnetcat及びipsendwinを搭載したPCを内部ネットワークに接続して、通信中継サーバー(PC)に負荷をかけ、TOEが機能不全にならないことをTOEの動作で確認する。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者によって悪用可能な潜在的な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

4　認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本ST及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL2に対する保証要件を満たすものと判断する。

5.2 注意事項

本評価においては、本TOEは「2.1.5 構成条件」に示した構成で評価されている。なお、本TOEのインストールプログラムは、インストール対象のOSに.NET Framework再頒布可能パッケージが存在するかどうかをチェックし、存在する場合には本TOEと共に再頒布される「Microsoft .NET Framework 2.0再頒布可能パッケージ」をインストールしない仕様になっている。このため、インストール対象のOSに、利用者が事前に.NET Framework再頒布可能パッケージを入手してインストールしている場合には、評価された構成とは異なる構成になる場合があるので注意が必要である。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation (セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation (セキュリティ評価方法)
EAL	Evaluation Assurance Level (評価保証レベル)
PP	Protection Profile (プロテクションプロファイル)
ST	Security Target (セキュリティターゲット)
TOE	Target of Evaluation (評価対象)
TSF	TOE Security Functionality (TOEセキュリティ機能)

本報告書で使用されたTOEに関する略語を以下に示す。

FX	Fuji Xerox Co., Ltd. (富士ゼロックス株式会社)

本報告書で使用された用語の定義を以下に示す。

Edgeサーバー	EPセンターに設置され、インターネットを介してEPセンターに送られてくる情報を受けるフロントエンドの役割をするサーバー。TOEの通信先となる。
EPサービス	FXの複合機を購入した利用者に対して、FXが提供する下記サービスの総称。「EP」はElectronic Partnershipの略。 1) 事務サービス 複合機のメーター値を定期的にEPセンターに送信することにより、利用者がメーター値を通知する手間をなくす。 2) 物流サービス 複合機の消耗品情報(Near Empty/Near Full等)を自動的にEPセンターに送信することにより、利用者が消耗品の追加注文を連絡する手間をなくす。 3) 保守サービス 複合機の障害情報をEPセンターに送信することにより、保守員の保守作業を支援する。
EPセンター	EPサービスを提供するために、FXが管理運用しているセンター。インターネットを介して、複合機からEPサービスのための情報を収集する。
EP通信データ	EPサービスのために、EP-BB機能搭載複合機から、TOEを経由してEPセンターに送信されるデータ。
EP-BB機能	設置先の内部ネットワークから、外部ネットワーク経由で

	EPセンターと通信する機能。「EP-BB」はElectronic Partnership - Broad Bandの略。
EP-BB機能搭載複合機	EP-BB機能を搭載した複合機。EPサービスの適用対象。
FXプロダクト認証局	FXが管理運用している認証局。インターネットを介して、TOE及びEP-BB機能搭載複合機に証明書を発行する。
外部ネットワーク	内部ネットワーク以外のネットワーク。インターネットが含まれる。
管理者	TOEを管理する利用者側の管理者。管理保守クライアント(PC)のWebブラウザを使用して、TOEの各種設定を行う特別な権限を持つ。管理者は、TOEが接続される内部ネットワークの管理も行う。
管理保守クライアント(PC)	TOEの管理と保守を実施する際に使用されるWebブラウザを搭載したPC。管理者によって管理されている。
通信中継サーバー(PC)	TOEを搭載したPC。利用者のサイトに設置され、EP-BB機能搭載複合機からEPセンターへの通信を中継する。管理者によって管理されている。
内部ネットワーク	利用者のサイト内部のネットワーク。TOEが接続される。
複合機	複写機、プリンター、イメージスキャナ、ファクシミリ等の事務機器の機能を1つの筐体に収めた機器。
複合機管理者	EP-BB機能搭載複合機を管理する利用者側の管理者。複合機の各種設定を行う特別な権限を持つ。
プロキシサーバー	内部ネットワークのコンピュータに代わって、「代理」として外部ネットワークとの接続を行うソフトウェア、あるいはソフトウェアを搭載したハードウェア。
保護エリア	許可された利用者のみが入場可能な場所。
保守員	TOEの障害対応をするFXまたはFX関連会社の従業員。管理保守クライアント(PC)のWebブラウザを使用して、TOEの各種設定を行う特別な権限を持ち、さらに保守用のログを取得することができる。
メーター値	複合機を使用して出力した印刷物のうち、情報が文字・画像として紙面に定着している面の数を測定した値。

7 参照

[1] EP通信集約サーバーソフトウエア セキュリティーターゲット バージョン 1. 26 2008年11月14日 富士ゼロックス株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 1 September 2006 CCMB-2006-09-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-002 (平成19年3月翻訳第1.2版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-003 (平成19年3月翻訳第1.2版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 1 September 2006 CCMB-2006-09-004

[12] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-004 (平成19年3月翻訳第1.2版)

[13] 富士ゼロックス株式会社 EP通信集約サーバーソフトウエア 評価報告書 第2.8版 2008年11月18日 有限責任中間法人 ITセキュリティセンター 評価部